MEMORANDO DE ENTENDIMENTO ENTRE
O GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA FEDERATIVA DO BRASIL
E
O ESCRITÓRIO DE COMUNIDADE ESTRANGEIRA E DESENVOLVIMENTO DO REINO UNIDO DA GRÃ-BRETANHA E IRLANDA DO NORTE
PARA COOPERAÇÃO NA ÁREA DE SEGURANÇA CIBERNÉTICA

O Gabinete de Segurança Institucional da República Federativa do Brasil e O Escritório de Comunidade Estrangeira e Desenvolvimento do Reino Unido da Grã-Bretanha e Irlanda Do Norte são referidos a seguir individualmente como a "Parte" e conjuntamente como as "Partes";

Considerando que governos, empresas e consumidores estão cada vez mais confrontados com uma variedade de ameaças cibernéticas e que é necessário melhorar ainda mais a prontidão para a segurança dos computadores e aumentar a conscientização sobre a importância de manter os sistemas seguros e promover práticas e procedimentos de segurança;

Reconhecendo que o ritmo e o desenvolvimento de novas tecnologias e aplicativos, em conjunto com o maior número de acessos, oferecem oportunidades significativas para o desenvolvimento econômico e social;

Tendo em conta que a dependência de redes cada vez mais interconectadas também expõe os Estados a novas vulnerabilidades, causando um profundo impacto no bem-estar das sociedades;

Reafirmando nosso compromisso de promover um ambiente cibernético aberto, seguro, acessível, pacífico e interoperável, baseado no respeito aos direitos humanos e às liberdades fundamentais, conducentes ao desenvolvimento social e econômico;

Reconhecendo que a ameaça da criminalidade no espaço cibernético requer mais esforço com vistas a promover a cooperação entre todas as partes interessadas, dentro e fora das fronteiras nacionais;

Desejando desenvolver a cooperação entre as partes na área de segurança cibernética, consistente com suas respectivas leis, regras e regulamentos nacionais, suas obrigações internacionais e com base nos princípios de reciprocidade e benefício mútuo;

Reconhecendo a importância de expandir a cooperação bilateral no campo da segurança cibernética como um dos aspectos mais importantes da manutenção da

segurança internacional e nacional, com o objetivo de impedir atividades que danifiquem intencionalmente e substancialmente a disponibilidade ou a integridade geral da Internet;

As Partes concordaram com o seguinte entendimento:

ARTIGO 1
Princípios Básicos

As Partes confirmam sua intenção, de acordo com este Memorando de Entendimento (MoU), de promover cooperação mais estreita e intercâmbio de informações referentes à segurança cibernética, criando parceria que reflita os valores compartilhados, as tradições democráticas, os direitos humanos, o estado de direito, a segurança nacional e o desenvolvimento econômico das Partes.

Este Memorando de Entendimento não cria, mantêm ou impõe quaisquer obrigações, direitos ou benefícios juridicamente vinculantes entre as Partes ou entre as Partes e terceiros.

Este Memorando de Entendimento deve ser implementado de acordo com as leis, os regulamentos, as políticas e as obrigações internacionais das Partes.

As Partes estão comprometidas em promover a segurança e a estabilidade no espaço cibernético, reconhecendo a aplicabilidade do direito internacional, em particular a Carta das Nações Unidas, à conduta responsável dos Estados no espaço cibernético e à promoção de normas voluntárias de comportamento responsável do Estado no espaço cibernético.

As Partes entendem a necessidade de trabalhar em estreita colaboração com o setor privado e com os parceiros de negócios, principalmente com aqueles considerados como infraestruturas críticas, reconhecendo que grande parte da inovação e do investimento que molda o espaço cibernético ocorre dentro das empresas privadas e que as múltiplas dimensões da segurança cibernética exigem cooperação entre governos e seus respectivos setores privados.

ARTIGO 2
Escopo da Cooperação

O escopo da cooperação entre as Partes deve incluir áreas relacionadas à segurança cibernética com as quais as Partes possam concordar mutuamente, como as seguintes:

a) Compartilhar experiências na regulamentação e pontos de vista sobre estratégias, políticas e melhores práticas nacionais sobre segurança cibernética;
b) Analisar e compartilhar experiências sobre legislação, com vistas a melhorar a cooperação jurídica bilateral e internacional, promovendo cooperação mais estreita entre órgãos e entidades para combater os crimes cibernéticos entre as Partes;
c) Promover medidas para facilitar o intercâmbio de informações sobre crimes cibernéticos, de acordo com as respectivas legislações nacionais;
d) Promover a cooperação entre órgãos públicos para combater atos e ameaças cibernéticas, inclusive por meio de oficinas de treinamento, aprimorando o diálogo e os processos, especialmente sobre forense digital e estruturas legais, e estabelecendo consultas conforme necessário;
e) Melhorar a capacidade de órgãos e entidades, equipando-os para redigir solicitações apropriadas de provas eletrônicas, de acordo com as respectivas leis e regulamentos;
f) Promover a troca de informações entre as equipes governamentais relevantes de resposta a incidentes de segurança de computadores em relação a incidentes cibernéticos ativos que afetam o Reino Unido e o Brasil usando os pontos de contato do FIRST.org.

g) Compartilhar as melhores práticas de avaliação, de desenvolvimento e de implementação de padrões para a segurança cibernética e para mecanismos de certificação, bem como fortalecer a segurança de processos, de produtos e de serviços digitais, durante todo o seu ciclo de vida e a sua cadeia de suporte;
h) Promover a cooperação nos domínios da educação, sensibilização, formação, capacitação e intercâmbio de conhecimentos entre especialistas;

i) Considerar oportunidades para coordenar esforços de pesquisa e desenvolvimento para melhorar a segurança cibernética e promover a interação acadêmica;
j) Estabelecer mecanismo institucional para troca periódica de pontos de vista sobre questões pendentes relacionadas aos incidentes cibernéticos e às ameaças atuais; e

k) Discutir e compartilhar estratégias para promover a integridade da cadeia de suprimento, a fim de aumentar a confiança dos usuários na segurança dos produtos e dos serviços de TIC.

ARTIGO 3
Implementação

A fim de implementar o escopo de cooperação identificado no artigo 2, as Partes comprometem-se a viabilizar o seguinte programa:

(a) Identificar oportunidades para discutir incidentes de segurança cibernética de interesse mútuo (por exemplo, ataques de negação de serviço, phishing, ataques de varredura graves e falsificação/desfiguração de sites governamentais);

(b) Apoiar-se mutuamente na tomada de medidas apropriadas, a fim de evitar a recorrência de tais incidentes de segurança cibernética e aprimorar seus esforços para aumentar o compartilhamento de informações sobre ameaças;

(c) Compartilhar avaliações da tendência prevalecente de segurança cibernética, conforme observado por cada país, periodicamente;

(d) Organizar visitas de representantes de ambas as Partes, para discutir questões atuais sobre segurança cibernética. Continuar a realizar discussões bilaterais regulares;

(e) Convidar representantes de governo, bem como representantes do setor privado, da academia e da sociedade, para seminários ou para conferências realizados nos respectivos países para discutir questões de segurança cibernética;

(f) Quaisquer outras áreas de cooperação relacionadas à segurança cibernética que possam ser mutuamente acordadas.

ARTIGO 4
Ponto de Contato

1. Com o objetivo de identificar e facilitar o programa previsto no artigo 3, as Partes designarão representantes para manter contato entre si. Os pontos de contato designados serão responsáveis por obter a aprovação necessária para a realização de atividades cooperativas específicas de seus respectivos governos.

2. Os representantes das Partes responsáveis pela implementação do escopo de cooperação, conforme estabelecido no Artigo 2 acima, poderão realizar consultas para identificar e definir atividades futuras previstas ou relacionadas no Artigo 3 e revisar atividades em andamento ou discutir assuntos relacionados a essas

atividades. Quando necessário, e de acordo mútuo, as Partes poderão realizar reuniões de trabalho alternadamente no Brasil e no Reino Unido, em datas mutuamente acordadas.

3. Os representantes designados para o Reino Unido da Grã-Bretanha e Irlanda do Norte serão o Chefe Adjunto da Missão do Reino Unido na República Federativa do Brasil e o Cyber Lead do Escritório de Comunidade Estrangeira e Desenvolvimento do Reino Unido da Grã-Bretanha e Irlanda Do Norte para a América do Sul.

4. Os representantes designados pela República do Brasil serão o Chefe Adjunto de Missão da República do Brasil no Reino Unido e o Diretor do Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República do Brasil.

ARTIGO 5
Formas de Cooperação

1. Todas as atividades de cooperação nos termos dos artigos 2, 3 e 4 deste Memorando de Entendimento serão conduzidas de acordo com as leis, regras e regulamentos aplicáveis de cada país.

2. Todas as atividades de cooperação previstas nos artigos 2, 3 e 4 deste Memorando de Entendimento estarão sujeitas à disponibilidade de fundos e outros recursos das Partes.

3. Para executar as atividades de cooperação estabelecidas neste Memorando de Entendimento, convidados do setor privado, equipes de tratamento e resposta a incidentes de redes, sociedade civil e academia poderão ser autorizados a participar, se acordado mutuamente pelas Partes.

ARTIGO 6
Direito de Propriedade Intelectual

1. Cada parte garantirá a proteção adequada dos Direitos de Propriedade Intelectual (doravante referidos como DPI) gerados a partir da cooperação nos termos deste Memorando de Entendimento em conformidade com suas respectivas leis, normas, regulamentos e acordos internacionais dos quais ambas as Partes são signatárias.

2. As Partes não cederão nenhum direito e obrigação decorrente do DPI gerado a invenções ou atividades realizadas sob este Memorando a terceiros sem o consentimento da outra Parte.

ARTIGO 7
Divulgação da informação

Nenhuma das Partes divulgará nem distribuirá a terceiras quaisquer informações transmitidas pela outra Parte no processo de atividades cooperativas sob este Memorando de Entendimento, exceto com o consentimento prévio por escrito da outra Parte.

ARTIGO 8
Resolução de Litígios

Toda e qualquer disputa entre as Partes relativa à interpretação e / ou implementação deste Memorando de Entendimento será resolvida amigavelmente por meio de consultas e / ou negociações entre as Partes.

ARTIGO 9
Entrada em vigor, duração, rescisão e alterações

1. Este Memorando de Entendimento entra em vigor imediatamente após a assinatura de ambas as Partes.

2. O presente Memorando de Entendimento permanecerá em vigor por período indeterminado.

3. Este Memorando de Entendimento pode ser alterado por consentimento mútuo por escrito das Partes, que será formalizado por meio de canais diplomáticos. A entrada em vigor das emendas ao presente Memorando de Entendimento estará sujeita ao mesmo procedimento utilizado para a entrada em vigor do Memorando de Entendimento.

4. A rescisão deste Memorando de Entendimento não afetará as atividades de cooperação nos termos dos Artigos 2 e 3, que já estiverem em andamento e até sua conclusão, a menos que as Partes determinem, por escrito, o contrário.

Em testemunho do que, os abaixo assinados, devidamente autorizados por suas respectivas Partes, assinaram este Memorando de Entendimento.

O registro anterior representa os entendimentos alcançados entre o Escritório de Comunidade Estrangeira e Desenvolvimento do Reino Unido da Grã-Bretanha e Irlanda Do Norte e o Gabinete de Segurança Institucional da Presidência da República do Brasil sobre os assuntos nele referidos.

Assinado em Londres, Reino Unido, no dia 21 de novembro de 2022, em dois originais, cada um nos idiomas português e inglês, sendo ambos os textos igualmente autênticos. Em caso de divergência de interpretação, o texto em inglês prevalecerá.

Assinado por e em nome do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil

Antônio Carlos de Oliveira Freitas
Assessor Especial de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República Federativa do Brasil


assinatura

21 NOVEMBRO 2022
data

Assinado por e em nome do Escritório de Comunidade Estrangeira e Desenvolvimento do Reino Unido da Grã-Bretanha e Irlanda Do Norte

William Middleton
Chefe do Departamento de Política Cibernética do Escritório de Comunidade Estrangeira e Desenvolvimento do Reino Unido da Grã-Bretanha e Irlanda Do Norte


assinatura

21 November 2022
data